Annex A:
Approved Security Functions for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

February 19, 2003
Draft

Jean Campbell
Randall J. Easter
Annabelle Lee
Ray Snouffer

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Annex A: Approved Security Functions for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

1. Introduction

Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of the cryptographic module. These areas include the following:

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)
9. Self Tests
10. Design Assurance
11. Mitigation of Other Attacks

The Cryptographic Module Validation Program (CMVP - www.nist.gov/cmvp) validates cryptographic modules to FIPS PUB 140-2 and other cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE - www.cse-cst.gc.ca) of the Government of Canada. Products validated as conforming to FIPS PUB 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated information (Canada).

In the CMVP, vendors of cryptographic modules use independent, accredited testing laboratories to have their modules tested. Organizations wishing to have validations performed would contract with the laboratories for the required services.

2. Purpose

The purpose of this document is to provide a list of the FIPS Approved security functions applicable to FIPS PUB 140-2.

Table of Contents

ANNEX A: APPROVED SECURITY FUNCTIONS

Annex A provides a list of the FIPS Approved security functions applicable to FIPS PUB 140-2. The categories include symmetric key, asymmetric key, message authentication and hashing.

Symmetric Key

1. **AES**

   National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001.

   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Special Publication 800-38A, December 2001.

2. **DES and Triple-DES**

   National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, October 25, 1999.

   National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, December 2, 1980.

   a. *DES Modes of Operation*, Change 2, May 31, 1996

   b. *DES Modes of Operation*, Change 3

   c. NIST Special Publication 800-38A Appendix E references Modes of Triple-DES.

   American Bankers Association, *Triple Data Encryption Algorithm Modes of Operation,* ANSI X9.52-1998.

3. **Skipjack**

   National Institute of Standards and Technology, Escrowed Encryption Standard (EES), Federal Information Processing Standards Publication 185, February 9, 1984.

   Skipjack and KEA Algorithm Specifications, Version 2.0, May 29, 1998.

Asymmetric Key

1. **DSA, RSA and ECDSA**

   National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000.

   American Bankers Association, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),* ANSI X9.31-1998.

   American Bankers Association, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),* ANSI X9.62-1998.

Message Authentication

1. **DES MAC and Triple-DES MAC**

   National Institute of Standards and Technology, *Computer Data Authentication*, Federal Information Processing Standards Publication 113, 30 May 1985.

2. **Enhanced Security DES MAC**

   American Bankers Association, *Financial Institution Retail Message Authentication*, ANSI X9.19-1996.

Hashing

1. Secure Hash Algorithm (SHA-1)

National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-1, April 17, 1995.

Keyed Hash

1. HMAC - Keyed-Hash Message Authentication Code

National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards Publication 198, March 06, 2002.

End of Document